One-time pad booster for Internet

Geraldo A. Barbosa*
QuantaSec – Research in Quantum Cryptography Ltd.,
1558 Portugal Ave., Belo Horizonte MG 31550-000 Brazil.

(Dated: 11 April 2007)

One-time pad encrypted files can be sent through Internet channels using current Internet protocols. However, the need for renewing shared secret keys make this method unpractical. This work shows how users can use a fast physical random generator based on fluctuations of a light field and the Internet channel to directly boost key renewals. The transmitted signals are deterministic but carries imprinted noise that cannot be eliminated by the attacker. Thus, a one-time pad for Internet can be made practical. Security is achieved without third parties and not relying on the difficulty of factoring numbers in primes. An informational fragility to be avoided is discussed. Information-theoretic analysis is presented and bounds for secure operation are determined.

PACS 89.70.+c,05.40.Ca,42.50.Ar,03.67.Dd

Unconditionally secure one-time pad encryption [1] has not find wide applicability in modern communications. The difficult for users to share long streams of secret keys beforehand has been an unsurmountable barrier preventing widespread use of one-time pad systems. Even beginning with a start sequence of shared secret keys, no amplification method to obtain new key sequences or key "refreshing" is available. This work proposes a practical solution for this problem and discusses its own limitations.

Assume that (statistical) physical noise $\mathbf{n} = n_1, n_2, ...$ has been added to a message bit sequence $\mathbf{X} = x_1, x_2, ...$ according to some rule $f_j(x_j, n_j)$ giving $\mathbf{Y} = f_1(x_1, n_1), f_2(x_2, n_2), ...$ (Whenever binary physical signals are implied, use $f_j(x_j, n_j)$ will represent $f_j = \oplus$ (=addition mod2)). When analog physical signals are made discrete by analog-to-digital converters, a sum of a binary signal onto a discrete set will be assumed). The addition process is performed at the emitter station and $\mathbf{Y}$ becomes a binary file carrying the recorded noise. $\mathbf{Y}$ is sent from user A to user B (or from B to A) through an insecure channel. The amount of noise is assumed high and such that without any knowledge beyond $\mathbf{Y}$, neither B (or A) or an attacker E could extract the sequence $\mathbf{X}$ with a probability P better than the guessing level of $P = (1/2)^N$, where N is the number of bits.

Assuming that A and B share some knowledge beforehand, the amount of information between A (or B) and E differs. Can this information asymmetry be used by A and B to share secure information over the Internet? It will be shown that if A and B start sharing a secret key sequence $\mathbf{K}_0$ they may end up with a practical new key sequence $\mathbf{K} \gg \mathbf{K}_0$. The security of this new sequence is discussed including an avoidable fragility for a-posteriori attack with a known-plaintext attack. Within bounds to be demonstrated, this makes one-time pad encryption practical for fast Internet communications (data, image or sound). It should be emphasized that being practical does not imply that $\mathbf{K}_0$ or the new keys have to be open to the attacker after transmission. These keys have to be kept secret as long as encrypted messages have to be protected, as in a strict one-time pad. The system gives users A and B direct control to guarantee secure communication without use of third parties or certificates. Some may think of the method as an extra protective layer to the current Internet encryption protocols. The system operates on top of all IP layers and does not disturb current protocols in use by Internet providers. Anyway, one should emphasize that the proposed method relies on security created by physical noise and not just on mathematical complexities such as the difficulty of factoring numbers in primes. This way, its security level does not depend on advances in algorithms or computation.

Random events of physical origin cannot be deterministically predicted and sometimes are classified in classical or quantum events. Some take the point of view that a recorded classical random event is just the record of a single realization among all the possible quantum trajectories possible [2]. These classifications belong to a philosophical nature, and are not relevant to the practical aspects to be discussed here. However, what should be emphasized is that physical noise is completely different from pseudo noise generated in a deterministic process (e.g. hardware stream ciphers) because despite any complexity introduced, the deterministic generation mechanism can be searched, eventually discovered and used by the attacker.

Before introducing the communication protocol to be used, one should discuss the superposition of physical signals to deterministic binary signals. Any signal transmitted over Internet is physically prepared to be compatible with the channel being used. This way, e.g., voltage levels V_0 and V_1 in a computer may represent bits. These values may be understood as the simple encoding

$$V^{(0)} \Rightarrow \begin{cases} V_0 \rightarrow \text{bit } 0 \\ V_1 \rightarrow \text{bit } 1 \end{cases} \tag{1}$$

Technical noise, e.g. electrical noise, in bit levels V_0 and V_1 are assumed low. Also, channel noise are assumed with a modest level. Errors caused by these noises

are assumed to be possibly corrected by classical error-correction codes. Anyway, the end user is supposed to receive the bit sequence $\mathbf{X}$ (prepared by a sequence of V_0 and V_1) as determined by the sender. If one of these deterministic binary signals x_j is repeated over the channel, e.g. $x_1 = x$ and $x_2 = x$, one has the known property $x_1 \oplus x_2 = 0$. This property has to be compared to cases where a non-negligible amount of physical noise n_j (in analog or a discrete form) has been added to each emission. Writing $y_1 = f_1(x_1, n_1) = f_1(x, n_1)$ and $y_2 = f_2(x_2, n_2) = f_2(x, n_2)$ one has $f(y_1, y_2) =$ neither 0 or 1 in general. This difference from the former case where $x_1 \oplus x_2 = 0$ emphasizes the uncontrollable effect of the noise.

The $V^{(0)}$ encoding shown above allows binary values V_0 and V_1 to represent bits 0 and 1, respectively. These values are assumed to be determined without ambiguity. Instead of this unique encoding consider that *two* distinct encodings can be used to represent bits 0 and 1: Either $V^{(0)}$ over which $x_0^{(0)}$ and $x_1^{(0)}$ represent the two bits 0 and 1 respectively, or $V^{(1)}$, over which $x_1^{(1)} = x_0^{(0)} + \epsilon$ and $x_0^{(1)} = x_1^{(0)} + \epsilon$ ($\epsilon \ll 1$) represent the two bits 1 or 0 (in a different order from the former assignment). These encodings represent physical signals as, for example, phase signals.

Assume noiseless transmission signals but where noise n_j has been introduced or added to each j^{th} bit sent (This is equivalent to noiseless signals in a noisy channel). Consider that the user does not know which encoding $V^{(0)}$ or $V^{(1)}$ was used. With a noise level n_j superposed to signals in $V^{(0)}$ or $V^{(1)}$ and if $|x_0^0 - x_0^1| \gg n_j \gg \epsilon$, one cannot distinguish between signals 0 and 1 in $V^{(0)}$ and $V^{(1)} = V^{(0)} + \epsilon$ but one knows easily that a signal belongs either to the set (0 in $V^{(0)}$ or 1 in $V^{(1)}$) **or** to the set (1 in $V^{(0)}$ or 0 in $V^{(1)}$). Also note that once the encoding used is known, there is no question to identify between x_j and $x_j + \epsilon$. In this case, it is straightforward to determine a bit 0 or 1 because values in a single encoding are widely separated and, therefore, distinguishable. One may say that without information on the encoding used, the bit values cannot be determined.

Physical noise processes will be detailed ahead but this indistinguishability of the signals without basis information is the clue for A and B to share random bits over the Internet in a secure way. Physical noise has been used before in fiber-optics based systems using M-ry levels [3] to protect information ($\alpha\eta$ systems). However, the system proposed here is completely distinct from those $\alpha\eta$ systems and it is related to the key distribution system presented in [4].

A brief description of protocol steps will be made, before a theoretic-security analysis is shown and the system's limitations discussed. It was said that if A and B start sharing a secret key sequence $\mathbf{K_0}$ beforehand they may end up with a secure fresh key sequence $\mathbf{K}$ much longer than $\mathbf{K_0}$ ($\mathbf{K} \gg \mathbf{K_0}$). Assume that $\mathbf{K_0}$ gives encoding information, that is to say, which encoding ($V^{(0)}$ or $V^{(1)}$) is being used at the j^{th} emission. Assume that $\mathbf{K}_0 = k_1^{(0)}, k_2^{(0)}, ...$ has a length K_0 and that the user A has a physical random generator PhRG able to generate random bits *and* noise in continuous levels. A generates a random sequence $\mathbf{K}_1 = k_1^{(1)}, k_2^{(1)}, ...k_{K_0}^{(1)}$ (say, binary voltage levels) and a sequence of K_0 noisy-signals n (e.g., voltage levels in a continuum). The deterministic signal (carrying recorded noise) $\mathbf{Y}_1 = k_1^{(0)} \oplus f_1(k_1^{(1)}, n_1^{(1)}), k_2^{(0)} \oplus f_2(k_2^{(1)}, n_2^{(1)}), ...$ is then sent to B. Is B able to extract the fresh sequence $\mathbf{K}_1$ from $\mathbf{Y}_1$? B applies $\mathbf{Y}_1 \oplus \mathbf{K_0} = f_1(k_1^{(1)}, n_1^{(1)}), f_2(k_2^{(1)}, n_2^{(1)}), ...f_N(k_N^{(1)}, n_N^{(1)})$. As B knows the encoding used and the signals representing bits 0 or 1 in a given encoding are easily identifiable: $f_1(k_1^{(1)}, n_1^{(1)}) \rightarrow k_1^{(1)}, f_2(k_2^{(1)}, n_2^{(1)}) \rightarrow k_2^{(1)}, ...f_N(k_N^{(1)}, n_N^{(1)}) \rightarrow k_N^{(1)}$. B then obtains the new random sequence $\mathbf{K}_1$ generated by A.

Is the attacker also able to extract the same sequence $\mathbf{K}_1$? Actually, this was a one-time pad with $\mathbf{K}_0$ with added noise and, therefore, it is known that the attacker *cannot* obtain $\mathbf{K}_1$. The security problem arises for further exchanges of random bits, e.g. if B wants to share further secret bits with A.

Assume that B also has a physical random generator PhRG able to generate random bits and noise in continuous levels. B wants to send in a secure way a freshly generated key sequence $\mathbf{K}_2 = k_1^{(2)}, k_1^{(2)}, ...k_{K_0}^{(2)}$ from his PhRG to A. B record the signals $\mathbf{Y}_2 = k_1^{(1)} \oplus f_1(k_1^{(2)}, n_2^{(2)}), k_2^{(1)} \oplus f_2(k_2^{(2)}, n_2^{(2)}), ...$ and sends it to A. As A knows $\mathbf{K}_1$ he(or she) applies $\mathbf{Y}_2 \oplus \mathbf{K_1}$ and extracts $\mathbf{K}_2$. A and B now share the two new sequences $\mathbf{K}_1$ and $\mathbf{K}_2$. For speeding communication, even a simple rounding process to the nearest integer would produce a simple binary output for the operation $f_j(k_j, n_j)$. The security of this process will be shown ahead.

The simple description presented show a key distribution from A to B and from B to A, with the net result that A and B share the fresh sequences $\mathbf{K}_1$ and $\mathbf{K}_2$. These steps can be seen as a first distribution cycle. A could again send another fresh sequence $\mathbf{K}_3$ to B and so on. This repeated procedure provides A and B with sequences $\mathbf{K}_1, \mathbf{K}_2, \mathbf{K}_3, \mathbf{K}_4, ...$ This is the basic key distribution protocol for the system.

A last caveat should be made. Although the key sharing seems adequate to go without bounds, physical properties impose some constraints and length limitations. Besides these limitations, the key sequences shared should pass key reconciliation and privacy amplification steps [5] to establish security bounds to all possible E attacks. The length limitation arises from the physical constraints discussed as follows.

A and B use PhRGs to generate physical signals creating the random bits that define the key sequences $\mathbf{K}$ and

the continuous noise $\mathbf{n}$ necessary for the protocol. Being physical signals, precise variables have to discussed and the noise source well characterized. Interfaces will transform the physical signals onto binary sequences adequate for Internet transmission protocols. Optical noise sources can be chosen for fast speeds. PhRGs have been discussed in the literature and even commercial ones are now starting to be available. Without going into details one could divide the PhRG in two parts, one generating random binary signals and another providing noise in a continuous physical variable (e.g., phase of a light field). These two signals are detected, adequately formatted and can be added.

Taking the phase of a light field as the physical variable of interest, one could assume laser light in a coherent state with average number of photons $\langle n\rangle$ within one coherence time ($\langle n\rangle = |\alpha|^2 \gg 1$) and phase ϕ. Phases $\phi = 0$ could define the bit 0 while $\phi = \pi$ could define the bit 1. It can be shown [4] (see also ahead) that two non-orthogonal states with phases ϕ_1 and ϕ_2 ($\Delta\phi_{12} = |\phi_1 - \phi_2| \rightarrow 0$ and $\langle n\rangle \gg 1$) overlap with (unnormalized) probability

$$p_u \simeq e^{-(\Delta\phi_{12})^2/2\sigma_\phi^2} \ , \tag{2}$$

where $\sigma_\phi = \sqrt{2/\langle n\rangle}$ is the standard deviation measure for the phase fluctuations $\Delta\phi$. For distinguishable states, $p_u \rightarrow 0$ (no overlap) and for maximum indistinguishability $p_u = 1$ (maximum overlap). With adequate formatting $\phi_1 - \phi_2$ gives the spacing ϵ ($\Delta\phi_{12} = \epsilon$) already introduced. Eq. (2) with $\Delta\phi_{12}$ replaced by $\Delta\phi$ describes the probability for generic phase fluctuations $\Delta\phi$ in a coherent state of constant amplitude ($|\alpha| = \sqrt{\langle n\rangle}$ =constant) but with phase fluctuations.

The laser light intensity is adjusted by A (or B) such that $\sigma_\phi \gg \Delta\phi$. This guarantees that the recorded information in the files to be sent over the open channel is in a condition such that the recorded light noise makes the two close levels ϕ_1 and ϕ_2 indistinguishable to the attacker. In order to avoid the legitimate user to confuse 0s and 1s in a *single* basis, the light fluctuation should obey $\sigma_\phi \ll \pi/2$. These conditions can be summarized as

$$\frac{\pi}{2} \gg \sqrt{2/\langle n\rangle} \gg \Delta\phi \ . \tag{3}$$

This shows that this key distribution system depends fundamentally on physical aspects for security and not just on mathematical complexity.

The separation between bits in the same encoding is easily carried under condition $\pi/2 \gg \sqrt{2/\langle n\rangle}$. The condition $\sqrt{2/\langle n\rangle} \gg \Delta\phi$ implies that that set of bits 0–in encoding 0, and 1–in encoding 1 (set 1) cannot be easily identifiable and the same happens with sets of bit 1–in encoding 0, and bit 0–in encoding 1 (set 2). Therefore, for A, B and E, there are no difficulty to identify that a sent signal is in set 1 or 2. However, E does not know the encoding provided to A or B by their shared knowledge on the basis used. The question "What is the attacker's probability of error in bit identification without repeating a sent signal?" has a general answer using information theory applied to a binary identification of two states [6]: The average probability of error in identifying two states $|\psi_0\rangle$ and $|\psi_1\rangle$ is given by the Helstrom bound [6]

$$P_e = \frac{1}{2}\left[1 - \sqrt{1 - |\langle\psi_0|\psi_1\rangle|^2}\,\right] \ . \tag{4}$$

Here $|\psi_0\rangle$ and $|\psi_1\rangle$ are coherent states of light [7] with same amplitude but distinct phases

$$|\psi\rangle = |\alpha\rangle = ||\alpha|e^{-i\phi}\rangle = e^{-\frac{1}{2}|\alpha|^2}\sum_n \frac{\alpha^n}{\sqrt{n!}}|n\rangle \ , \tag{5}$$

defined at the PhRG. $|\psi_0\rangle$ define states in encoding 0, where bits 0 and 1 are given by

$$|\psi_0\rangle = \begin{cases} |\alpha\rangle, & \text{for bit } 0, \text{ and} \\ |-\alpha\rangle, & \text{for bit } 1 \ , \end{cases} \tag{6}$$

$|\psi_1\rangle$ define states in encoding 1, where bits 1 and 0 are given by

$$|\psi_1\rangle = \begin{cases} ||\alpha|e^{-i\frac{\Delta\phi}{2}}\rangle, & \text{for bit } 1, \text{ and} \\ ||\alpha|e^{-i\left(\frac{\Delta\phi}{2}+\pi\right)}\rangle, & \text{for bit } 0 \ , \end{cases} \tag{7}$$

where $|\phi_0 - \phi_1| = \Delta\phi$. $|\langle\psi_0|\psi_1\rangle|^2$ is calculated in a straightforward way and gives

$$|\langle\psi_0|\psi_1\rangle|^2 = e^{-2\langle n\rangle\left[1-\cos\frac{\Delta\phi}{2}\right]} \ . \tag{8}$$

For $\langle n\rangle \gg 1$ and $\Delta\phi \ll 1$,

$$|\langle\psi_0|\psi_1\rangle|^2 \simeq e^{-\frac{\langle n\rangle}{4}\Delta\phi^2} \equiv e^{-\Delta\phi^2/\left(2\sigma_\phi^2\right)} \ , \tag{9}$$

where $\sigma_\phi = \sqrt{2/\langle n\rangle}$ is the irreducible standard deviation for the phase fluctuation associated with the laser field.

One should remind that in the proposed system the measuring procedure is defined by the users A and B and *no* attack launched by E can improve the deterministic signals that were already available to him(her). Thus, the noise frustrating the attacker's success, cannot be eliminated or diminished by measurement techniques.

One should observe that each random bit defining the key sequence is once sent as a message by A (or B) and then resent as a key (encoding information) from B (or A) to A (or B). In both emissions, noise is superposed to the signals. In general, coherent signal repetitions implies that a better resolution may be achieved that is proportional to the number of repetitions r. This improvement in resolution is equivalent to a single measurement with a signal $r\times$ more intense. To correct for this single repetition $\langle n\rangle$ is replaced by $2\langle n\rangle$ in $|\langle\psi_0|\psi_1\rangle|^2$. The final probability of error results

$$P_e = \frac{1}{2}\left[1 - \sqrt{1 - e^{-\frac{\langle n\rangle}{2}\Delta\phi^2}}\,\right] \ . \tag{10}$$

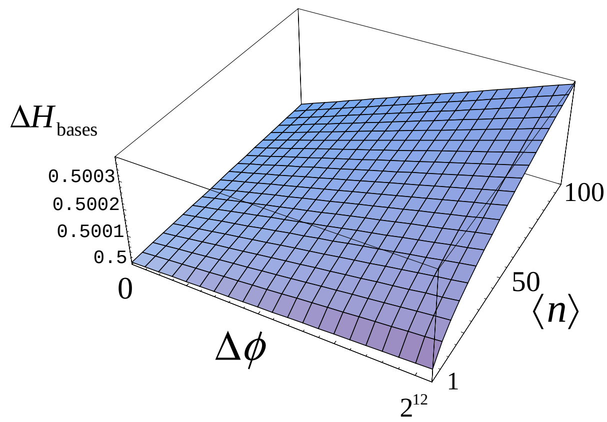

FIG. 1: ΔH_{bases} as a function of $\langle n \rangle$ and $\Delta\phi$.

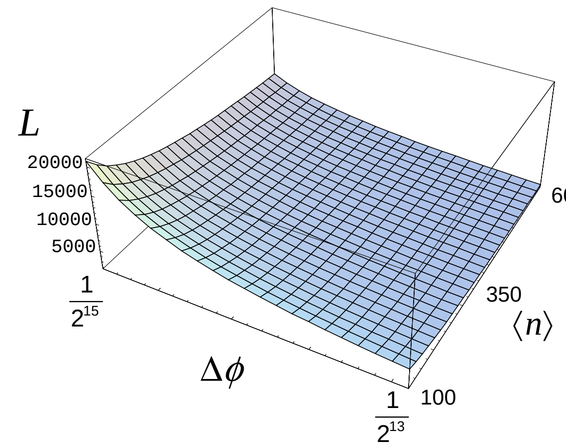

FIG. 2: Estimates for the minimum length of bits L exchanged between A and B that could give *one* bit of information about the bases used to the attacker.

This error probability can be used to derive some of the proposed system's limitations. The attacker's probability of success P_s $(= 1 - P_e)$ to obtain the basis used in a single emission may be used to compare with the a-priori starting entropy H_{bases} of the two bases that carry one bit of the message to be sent (a random bit). If the attacker knows the basis, the bit will also be known, with the same probability $\rightarrow 1$ as the legitimate user.

$$H_{\text{bases,bit}} = -p_0 \log p_0 - p_1 \log p_1 = 1 \ , \tag{11}$$

where p_0 and p_1 are the a-priori probabilities for each basis, $p_0 = p_1 = 1/2$, as defined by the PhRG. The entropy defined by success events is $H_s = -P_s \log P_s$. The entropy variation $\Delta H = H_{\text{bases,bit}} - H_s$, statistically obtained or leaked from bit measurements show the statistical information acquired by the attacker with respect to the a-priori starting entropy:

$$\Delta H_{\text{bases}} = \Big(H_{\text{bases,bit}} - H_s \Big) \ . \tag{12}$$

Fig. 1 shows ΔH_{bases} for some values of $\langle n \rangle$ and $\Delta\phi$. Value $\Delta H_{\text{bases}} = 1/2$ is the limiting case where the two bases cannot be distinguished. ΔH_{bases} deviations from this limiting value of $1/2$ indicates that some amount of information on the basis used may potentially be leaking to the attacker. It is clear that the attacker cannot obtain the basis in a bit-by-bit process. In order to be possible to obtain statistically a good amount of information on a single *one* encoding used, L should be given by

$$L \times \left(\Delta H_{\text{bases}} - \frac{1}{2} \right) \gg 1 \ . \tag{13}$$

Fig. 2 shows estimates for L for a range of values $\langle n \rangle$ and $\Delta\phi$ satisfying $L \times \left(\Delta H_{\text{bases}} - \frac{1}{2}\right) = 1$ ($\Delta\phi$ is given in powers of 2, indicating bit resolution for analog-to-digital converters).

It is assumed that error correction codes can correct for technical errors in the transmission/reception steps for the legitimate users. The leak estimate given by Eq. (13) do not imply that the information actually has leaked to the attacker. However, for security reasons, one takes for granted that this deviation indicate a statistical fraction of bits acquired by the attacker.

Privacy amplification procedures can be applied to the shared bits in order to reduce this hypothetical information gained by the attacker to negligible levels [5]. These procedures are beyond the purposes of the present discussion but one can easily accept that A and B may discard a similar fraction of bits to statistically reduce the amount of information potentially leaked. Reducing this fraction of bits after a succession of bits are exchanged between A and B implies, e.g., that the number of bits to be exchanged will decrease at every emission. Eventually, a new shared key $\mathbf{K}_0$ has to start the process again to make the system secure. Nevertheless, the starting key length K_0 was boosted in a secure way. Without further procedures, the physical noise allowed $\mathbf{K} \gg 10^3 \mathbf{K}_0$, a substantial improvement over the classical one-time pad factor of 1. One may still argue that the ultimate security relies on $\mathbf{K}_0$'s length because if $\mathbf{K}_0$ is known no secret will exist for the attacker. This is also true but does not invalidate the practical aspect of the system, because the $\mathbf{K}_0$ length can be made sufficiently long to frustrate any brute-force attack at any stage of technology. Therefore, the combination of physical noise and complexity makes this noisy-one-time pad practical for Internet uses.

Although the security of the process has been demonstrated, one should also point to a fragility of the system (without a privacy amplification stage) that has to be avoided when A and B are encrypting messages $\mathbf{X}$ between them. As it was shown, knowledge of one sequence of random bits lead to the knowledge of the following sequence. This makes the system vulnerable to know-plaintext attacks in the following way: E has a perfect

record of both sequences $\mathbf{Y}_1$ and $\mathbf{Y}_2$ and tries to recover any bit sequence from them, $\mathbf{K}_2$, $\mathbf{K}_1$ or $\mathbf{K}_0$. E will wait until A and B uses these sequences for encryption before trying to brake the system. A and B will encrypt a message using a new shared sequence, $\mathbf{K}_1$ or $\mathbf{K}_2$. This message could be a plain-text, say $\mathbf{X} = x_1, x_2, ...x_{K_0}$ *known* to the attacker. Encrypting this message with say $\mathbf{K}_1$ in a noiseless way, gives $\mathbf{Y} = x_1 \oplus k_1^{(1)}, x_2 \oplus k_2^{(1)}, ...x_{K_0} \oplus k_{K_0}^{(1)}$. Performing the operation $\mathbf{Y} \oplus \mathbf{X}$, E obtains $\mathbf{K}_1$. The chain dependence of $\mathbf{K}_j$ on $\mathbf{K}_{j-1}$ creates this fragility. Even addition of noise to the encrypted file does not eliminate this fragility, because the attacker can use his/her knowledge of $\mathbf{X}$ –as the key– to obtain $\mathbf{K}$–as a message. The situation is *symmetric* between B or the attacker: one that knows the key ($\mathbf{X}$ for E, and $\mathbf{K}$ for B) obtains the desired message ($\mathbf{K}$ for E, and $\mathbf{X}$ for B) [8] .

In general, random generation processes are attractive to attackers and have to be carefully controlled. Well identifiable physical components (e.g. PHRG) are usually a target for attackers that may try to substitute a true random sequence by pseudo-random bits generated by a seed key under his/her control. Electronic components can also be inserted to perform this task replacing the original generator; electric or electromagnetic signal may induce sequences for the attacker and so on. In the same way, known-plaintext attacks also have to be carefully avoided by the legitimate users. The possibility of further privacy amplification procedures to eliminate the known-plaintext attack presented is beyond the purposes of this work.

Many protocols that use secret key sharing may profit from this one-time pad booster system. For example, besides data encryption, authentication procedures can be done by hashing of message files with sequences of shared secret random bits. Challenge hand-shaking may allow an user to prove its identity to a second user across an insecure network.

As a conclusion, it has been shown that Internet users will succeed in generating and sharing, in a fast way, a large number of secret keys to be used in one-time-pad encryption as described. They have to start from a shared secret sequence of random bits obtained from a *physical* random generator hooked to their computers. The physical noise in the signals openly transmitted is set to hide the random bits. No intrusion detection method is necessary. Privacy amplification protocols eliminate any fraction of information that may have eventually obtained by the attacker. As the security is not only based on mathematical complexities but depend on physical noise, technological advances will not harm this system. This is then very different from systems that would rely entirely, say, on the difficulty of factoring large numbers in their primes. It was then shown that by sharing secure secret key sequences, one-time pad encryption over the Internet can be practically implemented.

*E-mail: GeraldoABarbosa@hotmail.com

[1] G. S. Vernam, J. Amer. Inst. Elec. Eng. **55**, 109 (1926). C. E. Shannon, Bell Syst. Tech. J. **28**, 656 (1949).

[2] V. P. Belavkin, Int. J. of Theoretical Physics **42**, 461 (2003).

[3] G. A. Barbosa, E. Corndorf, P. Kumar, H. P. Yuen, Phys. Rev. Lett. **90**, 227901 (2003). E. Corndorf, G. A. Barbosa, C. Liang, H. P. Yuen, P. Kumar, Opt. Lett. **28**, 2040 (2003). G. A. Barbosa, E. Corndorf, and P. Kumar, Quantum Electronics and Laser Science Conference, OSA Technical Digest **74**, 189 (2002).

[4] G. A. Barbosa, Phys. Rev. A **68**, 052307 (2003); Phys. Review A 71, 062333 (2005); quant-ph/0607093 v2 16 Aug 2006.

[5] S. Wolf, Information-Theoretically and Computationally Secure Key Agreement in Cryptography, PhD thesis, ETH Zurich 1999.

[6] C. W. Helstrom, Quantum Detection and Estimation Theory, ed. R. Bellman (Academic Press, 1976), pg. 113 Eq. (2.34).

[7] R. J. Glauber, Phys. Rev. **130**, 2529 (1963); Phys. Rev. **131**, 2766 (1963); Quantum Optics and Electronics, eds. C. DeWitt, A. Blandin, C. Cohen-Tannoudji (Dunod, Paris 1964), Proc. École d'Été de Physique Théorique de Les Houches, 1964.

[8] The author thanks one of the reviewers for a demonstration of this fragility.